CLAIMS

1. A method, comprising:

selecting multiple data sources connected to an identity integration system; and

performing a password operation on a password associated with at least one of the multiple data sources, wherein the password operation is performed using the identity integration system.

2. The method as recited in claim 1, further comprising:

determining an identity of a user, wherein the multiple data sources are associated with the identity; and

querying the identity integration system to find the multiple data sources associated with the identity.

3. The method as recited in claim 1, wherein the password operation comprises updating one or more passwords associated with the multiple data sources using joined objects across the multiple data sources, wherein the joined objects are stored in the identity integration system.

4. The method as recited in claim 3, wherein some of the multiple passwords are updated to new passwords that differ from each other.

5. The method as recited in claim 3, wherein each of the multiple passwords is updated to the same password.

6. The method as recited in claim 1, wherein the password operation comprises one of changing, setting and resetting the password.

7. The method as recited in claim 1, wherein each of the multiple data sources differ from others of the multiple data sources with respect to at least one of a protocol, a platform, a format, and a data transmission medium for data storage.

8. The method as recited in claim 1, wherein each of the multiple data sources differs in a connection to the identity integration system with respect to at least one of a protocol, a platform, a format, and a data transmission medium for data storage.

9. The method as recited in claim 1, wherein each of the multiple data sources uses a different password management function.

10. The method as recited in claim 9, wherein the identity integration system performs password management for each of the multiple data sources.

11. The method as recited in claim 1, wherein for at least some of the multiple data sources the identity integration system stores integrated identity information to perform password management.

12. The method as recited in claim 1, wherein the identity integration system includes a management agent for each of the multiple data sources to manage data communication between the identity integration system and each respective data source, and wherein for at least some of the multiple data sources a management agent for the data source is configured with credentials to perform password management.

13. The method as recited in claim 12, wherein the identity integration system includes a management agent for each of the multiple data sources to manage data communication between the identity integration system and each respective data source, and wherein for at least one of the multiple data sources a management agent for the data source calls for custom logic to perform password management for the data source.

14. The method as recited in claim 13, wherein the management agent calls for custom logic from a custom logic source outside the identity integration system.

15. The method as recited in claim 1, further comprising using the identity integration system to produce a list of user accounts associated with the multiple data sources, wherein the user accounts on the list are eligible for password management.

16. The method as recited in claim 1, further comprising allowing access to the identity integration system through a web application for password management.

17. The method as recited in claim 16, wherein the selecting multiple data sources and the performing a password operation are performed on a website generated by the web application.

18. The method as recited in claim 17, wherein the web application accepts a password credential from a user to perform the password operation.

19. The method as recited in claim 17, wherein the web application verifies an identity of a user by asking the user questions, wherein if answers provided by the user are correct then the web application performs the password operation using the identity of a privileged user account.

20. The method as recited in claim 17, further comprising using the identity integration system to produce a list of user accounts displayable on the website, wherein the user accounts are associated with the multiple data sources.

21. The method as recited in claim 17, further comprising a help desk to at least assist in the performing a password operation.

22. The method as recited in claim 17, further comprising communicatively coupling the identity integration system with the web application using an interface.

23. The method as recited in claim 22, wherein the interface is publicly available.

24. The method as recited in claim 22, wherein the interface allows a web application designer to customize the web application.

25. The method as recited in claim 22, wherein the interface includes password management functions.

26. The method as recited in claim 22, wherein the interface is capable of being changed for an improved version of the interface that adds more password management functions while using the same web application and the same identity integration system.

27. The method as recited in claim 22, wherein the interface is a WINDOWS MANAGEMENT INSTRUMENTATION interface.

28. The method as recited in claim 27, wherein the interface is secured using a security group.

29. The method as recited in claim 28, wherein the interface is secured using a security group that allows both searching for a connector object associated with a data source and setting a password for an object in the data source, wherein a connector object represents at least part of the data source in the identity integration system.

30. The method as recited in claim 1, wherein an identity of a user associated with the multiple data sources provides a security credential for performing a password operation.

31. The method as recited in claim 17, wherein the web application produces a list of accounts associated with a user.

32. The method as recited in claim 31, wherein the web application lists only accounts eligible for password management.

33. The method as recited in claim 17, wherein the web application adopts a web application behavior based on a configuration setting.

34. The method as recited in claim 33, wherein the configuration setting is stored in a configuration file.

35. The method as recited in claim 17, wherein the web application checks if one of the data sources is communicating before updating a password associated with the data source.

36. The method as recited in claim 35, wherein the updating comprises one of changing and setting the password.

37. The method as recited in claim 17, wherein the web application checks if a connection to one of the data sources is secure before updating a password associated with the data source.

38. The method as recited in claim 37, wherein the updating comprises one of changing and setting the password.

39. The method as recited in claim 1, further comprising displaying a status for the password operation.

40. The method as recited in claim 39, further comprising displaying the status on a webpage.

41. The method as recited in claim 1, further comprising auditing the password operation.

42. The method as recited in claim 41, further comprising maintaining a password management history for the password operation.

43. The method as recited in claim 42, further comprising keeping the password management history in a connector space object, wherein the connector space object is included in the identity integration system.

44. The method as recited in claim 42, wherein the password management history includes a tracking identifier to an audit record of the password operation.

45. The method as recited in claim 41, further comprising maintaining a repository of audit records for password operations performed using the identity integration system.

46. The method as recited in claim 45, wherein an audit record for a password operation includes at least one of an identifier of a user associated with the password operation, a tracking identifier to a web application initiating the password operation, a tracking identifier to a connector object associated with the password operation, a tracking identifier to a management agent associated with the password operation, a password operation identifier, a password operation status, a date, and a time.

47. The method as recited in claim 1, further comprising associating custom logic with a password operation, wherein the custom logic is executed after the password operation is performed.

48. The method as recited in claim 47, wherein the custom logic sends an email.

49. The method as recited in claim 47, wherein the custom logic logs password management activity.

50. The method as recited in claim 47, wherein the custom logic performs a password operation on a subsequent data source not connected to the identity integration system.

51. The method as recited in claim 1, wherein the password operation further comprises updating passwords in both secure and non-secure data sources within the multiple data sources.

52. The method as recited in claim 1, wherein the password operation further comprises updating passwords over both secure and non-secure connections to the multiple data sources.

53. A web application for password management, comprising:

a user identifier to find user identity information in an identity integration system;

identity information query logic to search information in the identity integration system for accounts associated with the user;

an account lister to display the accounts associated with the user;

an account selector to designate at least some of the displayed accounts for password management;

a password inputter to determine a new password; and

a password manager to request an update of a password associated with an account.

54. The web application as recited in claim 53, wherein the identity integration system connects with diverse data sources, each data source having a different function for using password security.

55. The web application as recited in claim 53, further comprising an account status display to show selected accounts and a connection status of each account.

56. The web application as recited in claim 53, further comprising a password management status display to display a password management operation status for each account.

57. The web application as recited in claim 53, further comprising a status checker to verify connectivity and security of a connection between an account and the identity integration system.

58. The web application as recited in claim 53, further comprising a configuration reader to obtain behavior settings for the web application.

59. The web application as recited in claim 53, further comprising a custom logic executor to perform custom logic associated with a password management operation.

60. The web application as recited in claim 53, wherein the account lister lists only accounts eligible for password management.

61. An interface for coupling an identity integration system with a password management web application, comprising:

logic for communicating with the identity integration system, wherein the identity integration system is capable of updating a password on data sources that use various functions of password updating;

logic for communicating with the password management web application;

logic for searching for objects in the identity integration system; and

logic for checking a connection status between the identity integration system and a data source.

62. The interface as recited in claim 61, further comprising logic for checking security of a connection between the identity integration system and a data source.

63. The interface as recited in claim 61, further comprising logic to change a password associated with the data source.

64. The interface as recited in claim 61, further comprising logic to set a password associated with the data source.

65. A password management system, comprising:

a identity integration system having a metaverse space for persisting integrated identity information regarding accounts associated with a user and a connector space for persisting information representing multiple data sources connectable to the identity integration system, wherein the accounts have associated manageable passwords;

a web application for producing a list of the accounts from the identity integration system, for allowing selection of at least some of the accounts, for inputting a password, and for requesting the identity integration system to update passwords on the accounts based on the input password; and

an interface to communicatively couple the identity integration system with the web application.

66. The password management system as recited in claim 65, wherein the password management web application verifies one of an identity and a credential of a user.

67. The password management system as recited in claim 65, wherein the web application generates a webpage that displays accounts and a status of a password management operation for each account displayed.

68. The password management system as recited in claim 65, wherein the web application operates in a security context.

69. The password management system as recited in claim 68, wherein the security context is an application pool identity.

70. The password management system as recited in claim 69, further comprising a help desk application, wherein the web application denies a user access to the help desk application if a security group of the user is not approved by the web application.

71. The password management system as recited in claim 65, wherein the identity integration system stores a password management operation history for each account.

72. The password management system as recited in claim 65, wherein the identity integration system communicates with diverse accounts, each account having a different mechanism for administering a password associated with the account.

73. The password management system as recited in claim 72, wherein the identity integration system does not natively communicate with at least some of the diverse accounts.

74. A management agent for an identity integration system, comprising:

logic for adapting a connection for data communication, wherein the connection couples an identity integration system using a first data communication format with a connected data source using a second data communication format; and

logic for requesting a connected data source to perform a password operation.

75. The management agent as recited in claim 74, wherein the management agent performs the password operation.

76. The management agent as recited in claim 74, wherein the management agent requests authorization for performing a password operation.

77. The management agent as recited in claim 74, wherein the management agent is configured with credentials to perform a password management operation.

78. The management agent as recited in claim 74, wherein the management agent is configured with credentials to request a password management operation.

79. The management agent as recited in claim 74, further comprising logic to perform a call out for custom logic for performing a custom password operation.

80. In a computer system having a graphical user interface including a display and a user interface selection device, a method of providing and selecting from a menu on the display comprising the steps of:

retrieving a list of user accounts from an identity integration system having persisted identity information regarding the user accounts;

showing the list of user accounts on the display;

allowing each account in the list to be selected using the user interface selection device;

allowing input of a new password via the user interface selection device; and

allowing input of a request to update old passwords associated with the selected accounts to the new password.

81. The method in the computer system having the graphical user interface as recited in claim 80, further comprising allowing input of user credentials to verify an identity of the user.

82. One or more computer readable media containing instructions that are executable by a computer to perform actions, comprising:

selecting multiple data sources connected to an identity integration system; and

for at least one of the multiple data sources, using the identity integration system to perform a password operation.

83. The one or more computer readable media as recited in claim 82, wherein at least some of the multiple data sources connected to the identity integration system communicate in a manner different than a native communication of the identity integration system.

84. The one or more computer readable media as recited in claim 82, wherein the identity integration system accomplishes a password update on each of the data sources regardless of whether the data sources connected to the identity integration system communicate in a manner different than a native communication of the identity integration system.

85. The one or more computer readable media as recited in claim 84, wherein the identity integration system accomplishes a password update on at least one of an ACTIVE DIRECTORY® data source, a SUN ONE server data source, a LOTUS NOTES server data source, a WINDOWS® NT™ server data source, a NOVELL® EDIRECTORY™ server data source, and a flat file data source.